UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/729,515	12/05/2003	Anoop Anantha	MS306116.1/MSFTP502US	2367

27195 7590 02/02/2009

AMIN, TUROCY & CALVIN, LLP
127 Public Square
57th Floor, Key Tower
CLEVELAND, OH 44114

EXAMINER
TRAORE, FATOUMATA

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
02/02/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket1@thepatentattorneys.com
hholmes@thepatentattorneys.com
lpasterchek@thepatentattorneys.com

Office Action Summary	Application No.	Applicant(s)	
	10/729,515	ANANTHA ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16 and 18-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6, 18-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed October 24, 2008. Claims 1 and 30-32 have been amended. Claim 17 has been cancelled. Claims 1-16 and 18-32 are pending and have been considered below.

Response to Arguments

2. Applicant's arguments filed 10/24/2008 have been fully considered but they are not persuasive.

3. Regarding claims 1-16 and 30-32 , the arguments have been considered but are moot in view of the new ground(s) of rejection.

4. Regarding claims 18-29, Applicant asserted that "Beckwith et al is silent regarding a security option which include at least conversion of a subscription from a first type associated with a first tenant to a second type associated with a second tenant, wherein the security option indicates allowability of the second tenant to convert the subscription type from the first type to the second type."

5. The examiner respectfully disagrees because of the following reasons:

First, Beckwith et al was used primarily for teaching "storing one or more security options".

As noted above, Corrigan et al discloses security options including at least conversion of a subscr4tion from a first type to a second type. See column 2, lines 5-7 and column 3, lines 19-24.

In addition, it should be noted that Corrigan et a! teaches "storing one or more security options". See column 2, lines 9-14.

Furthermore, it is submitted that Beckwith et al discloses a global service management system for an advanced intelligent network, wherein there is provided "a security option which include at least conversion of a subscription from a first type associated with a first tenant to a second type associated with a second tenant, wherein the security option indicates allowability of the second tenant to convert the subscription type from the first type to the second type". See column 3, lines 29-40; column 6, lines 5- 9; column 7, lines 54-56; column 8, lines 47-58; column 10 and 13.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 6 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beckwith et al (US 6,330,598) in view of Koritzinsky et al (US 6,272,469).

Claims 1 and 30: Beckwith et al discloses a system that facilitates access to a plurality of shared software objects by disparate entities, comprising:

i. a platform component that receives a request to access an object by a first entity, wherein the first entity is attempting to convert a

subscription from a second type of a second entity to a type of the first entity(*column 7, lines 54-60; column 8, line 9 lines 47-60)* ;

ii. a data store that stores security information on classes of the objects (*security database) (column 16, lines 9-20)*,

Beckwith et al does not explicitly discloses that the wherein the security information includes a security parameter that indicates allowability of the first entity to convert the subscription from the second type to the first type; nor a verification component that employs the security information to verify that the first entity has permission to call an Application Programming Interface (API) for the object or operate on the object to convert the subscription from the second type to the first type. However , Koritzinsky et al discloses an imaging system protocol handling method, which further discloses

i. wherein the security information includes a security parameter that indicates allowability of the first entity to convert the subscription from the second type to the first type(*column 21, line 33 to column 22 line 34);* and

ii. a verification component that employs the security information to verify that the first entity has permission to call an Application Programming Interface (API) for the object or operate on the object to convert the subscription from the second type to the first type(*column 22, lines 34 to column 23 line 15*).

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teaching of Beckwith et al such

as to indicate allowability to convert a subscription form a second to a first type. One would have been motivated to do in order to make the system flexible

Claim 6: Beckwith et al and Korizzinsky et al disclose a system that facilitates access to a plurality of shared software objects by disparate entities as in claim 1 above, and Beckwith et al further discloses that the data store provides a default or determined security information related to a class (Fig. 4, item 83).

8. Claims 2, 3 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beckwith et al (US 6,330,598) in view of Koritzinsky et al (US 6,272,469) in further view of Cheng (US 7,096,491).

Claim 2: Beckwith et al and Koritzinsky et al disclose et al discloses a system that facilitates access to a plurality of shared software objects by disparate entities as in claim 1 above, while neither of them explicitly discloses that the verification component exposes the object to the entity if permission exists. However, Cheng discloses a mobile code security architecture in an application service provider environment, which further discloses that the verification component exposes the object to the entity if permission exists(Fig. 3, item 136). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of combined teaching of Beckwith et al and Koritzinsky et such as to expose the object if permission exits. One would have been motivated to do in order to make the system secure.

Claim 3: Beckwith et al and Korizzinsky et al disclose a system that facilitates access to a plurality of shared software objects by disparate entities as in claim 1 above, while neither of them explicitly discloses that the verification component masks the object is permission does not exist. However, Cheng discloses a mobile code security architecture in an application service provider environment, which further discloses that the verification component masks the object is permission does not exist (Fig. 3, item 138). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of combined teaching of Beckwith et al and Koritzinsky et such as to mask the object if permission does not exit. One would have been motivated to do in order to make the system secure.

Claim 5: Beckwith et al and Koritzinsky et al disclose a system that facilitates access to a plurality of shared software objects by disparate entities as in claim 1 above, while neither of them explicitly discloses that the verification component facilitates that entity receive full access to Application Programming Interfaces (API's) and /or object s for which there is a business need and partial or limited access to other API's or business objects. However, Cheng discloses a mobile code security architecture in an application service provider environment, which further discloses that the verification component facilitates that entity receive full access to Application Programming Interfaces (API's) and /or object s for which there is a business need and partial or limited access to other API's or business objects (during subscription process, the user will grant the application privileges

to perform only those functions, and to access only those resource, needed for the English to Spanish translation) (column 4, lines 54-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of combined teaching of Beckwith et al and Koritzinsky et such as to limit access to the object. One would have been motivated to do in order to make the system secure.

9. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Beckwith et al (US 6,330,598) in view of Koritzinsky et al (US 6,272,469) in further view of Higley et al (US 5,913,025) .

Claim 8: Beckwith et al and Koritzinsky et al disclose a system that facilitates access to a plurality of shared software objects by disparate entities as in claim 1 above, while neither of them explicitly discloses that the system further comprising a proxy tenant component wherein an intermediate entity places calls into a subscription platform service on behalf of another entity and achieves access to selected objects in order for the another entity to complete a subscription purchase. However, Higley et al discloses a system of proxy authentication , which further discloses that the system further comprising a proxy tenant component wherein an intermediate entity places calls into a subscription platform service on behalf of another entity and achieves access to selected objects in order for the another entity to complete a subscription purchase (*column 10, lines 35-55).* Therefore, it would have been obvious to one

having ordinary skill in the art at the time the invention was made to modify the combined teaching of combined teaching of Beckwith et al and Koritzinsky et such as to support proxies tenant callers. One would have been motivated to do in order to make the system flexible.

10. Claims 4, 7 and 13-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beckwith et al (US 6,330,598) in view of Koritzinsky et al (US 6,272,469) in further view of Corrigan et al (US 6,640,097).

Claim 4: Beckwith et al and Koritzinsky et al disclose a system that facilitates access to a plurality of shared software objects by disparate entities as in claim 1 above, while neither of them explicitly discloses that the system further comprise a subscription platform to facilitate automated billing and provisioning accounts. However, Corrigan et al discloses a similar system, which discloses a subscription platform to facilitate automated billing and provisioning accounts (column 4, lines 45-50). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Beckwith et al and Koritzinsky et al such as to include a subscription platform to facilitating automated billing and provisioning accounts. One would have been motivated to do so in order to facilitate accounts management.

Claim 7: Beckwith et al and Koritzinsky et al disclose a system that facilitates access to a plurality of shared software objects by disparate entities as in claim 6

above, while neither of them explicitly discloses that the system further comprise a component to override the default security information with higher or different security options. However, Corrigan et al discloses a similar system, which further comprises a component to override the default security information with higher or different security options (from the generic subscriber class are derived many subscriber sub-class that allow the portal to manage subscriber profiles across a wide range of different technologies) (column 8, lines 47-50). I Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Beckwith et al and Koritzinsky et al such as to override default security with higher or different security options. One would have been motivated to do in order to make the system efficient.

Claim 13: Beckwith et al and Koritzinsky et al disclose a system that facilitates access to a plurality of shared software objects by disparate entities as in claim 1 above, while neither of them explicitly discloses that the system further comprises al least one of a sign-up API caller, an account management API caller, and a customer care API caller. However, Corrigan et al discloses a similar system, which further discloses a customer care-provisioning interface including a device provisioning function which enables the operator to ensure that content is matched to the device type (column 5, lines 10-15). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Beckwith et al and

Koritzinsky et al such as to include a customer care API caller. One would have been motivated to do in order to simplify service management.

Claim 14: Beckwith et al, Koritzinsky et al and Corrigan et al disclose a system that facilitates access to a plurality of shared software objects by disparate entities as in claim 13 above, Corrigan et al further discloses disclose that the system further comprises al least one API related to at least of a sign-up API group, an account management API group, a customer care API group, and object designer API group (to provide access control to individual properties that further a customer care provisioning interface including a device provisioning function which enables the operator to ensure that content is matched to the device type) (column 5, lines 10-15). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Beckwith et al and Koritzinsky et al such as to include a customer care API group. One would have been motivated to do in order to make the system efficient.

Claim 15: Beckwith et al and Koritzinsky et al disclose a system that facilitates access to a plurality of shared software objects by disparate entities as in claim 1 above, while neither of them explicitly discloses that the system further comprises an authorization logic that determines whether an API can access an object via an access rights set. However, Corrigan et al discloses a similar system, which further discloses that the system further comprises an authorization logic that determines whether an API can access an object via an

access rights set (to provide access control to individual properties that further discloses a node acting as a service manager for mobile subscriber. It controls all subscriber accesses to the network operators managed service portfolio and authenticates the subscriber ID to verify that the subscriber is authorized to access a particular service before opening a secure connection) (column 5, lines 35-40). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Beckwith et al and Koritzinsky et al such as to include an authorization component. One would have been motivated to do so in order to restrict and control access to various components and services provides within the system.

Claim 16: Beckwith et al and Koritzinsky et al discloses a system that facilitates access to a plurality of shared software objects by disparate entities as in claim 1 above, while neither of them explicitly discloses that the system further comprises at least one of a restricted audience offer, a conversion component, and a payment instrument component. However, Corrigan et al discloses a similar system, which further discloses that that the system further comprises at least one of a restricted audience offer, a conversion component, and a payment instrument (*to provide access control to individual properties that further discloses a payment management class from which are derived two sub-classes post-paid and pre-paid) (column 10, lines 20-25*). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Beckwith et al and Koritzinsky et al such as

to include a payment component. One would have been motivated to do so in order to restrict and control access to various components and services provides within the system.

11. Claims 9-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beckwith et al (US 6,330,598) in view of Koritzinsky et al (US 6,272,469) in further view of Garg et al (US 6,289,458).

Claim 9: Beckwith et al and Koritzinsky et al discloses a system that facilitates access to a plurality of shared software objects by disparate entities as in claim 1 above, while neither of them explicitly discloses a management portal to facilitate authorization. However Garg et al discloses a system to provide access control to individual properties of an object, which comprises a management portal to facilitate authorization (*file system manger maintains and coordinates access to file system) (column 7, lines 25-29*). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Beckwith et al and Koritzinsky et al such as to include a management portal. One would have been motivated to do so in order to help maintain the integrity of the system by not allowing changes to be made to the software by any entity, both known and unknown, scrupulous and unscrupulous.

Claim 10: Beckwith et al and Koritzinsky et al discloses a system that facilitates access to a plurality of shared software objects by disparate entities as in claim 1 above, while neither of them explicitly discloses a component to provide an

explicit security mapping for an object. However, Garg et al discloses a system to provide access control to individual properties of an object which, further comprises a component to provide an explicit security mapping for an object (*the access control list contains zero or more access control entries, which define the access control applied to the object. Each entry in the list defines a set of permission to be applied to a particular UUSERID or GROUPID with respect to either the object as a whole or individual properties of object. Desirably the order of entries in the access control list is significant) (column 8, lines 35-55*). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Beckwith et al and Koritzinsky et al such as to include a management portal. One would have been motivated to verify this in order to help maintain the integrity of the system by not allowing changes to be made to the software by any entity, both known and unknown, scrupulous and unscrupulous.

Claim 11: Beckwith et al and Koritzinsky et al discloses a system that facilitates access to a plurality of shared software objects by disparate entities as in claim 1 above, while neither of them explicitly discloses a component to enable an implicit security mapping from an explicit mapped object or to derive an implicit security permission by utilizing related objects. However, Garg et al discloses a system to provide access control to individual properties of an object as in claim 1, above and further comprises a component to enable an implicit security mapping from an explicit mapped object or to derive an implicit security

permission by utilizing related objects (*security descriptor provides details on the security and access control applicable to object (column 8, lines 25-30*). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Beckwith et al and Koritzinsky et al such as to include a management portal.. One would have been motivated to verify this in order to help maintain the integrity of the system by not allowing changes to be made to the software by any entity, both known and unknown, scrupulous and unscrupulous.

Claim 12: Beckwith et al and Koritzinsky et al discloses a system that facilitates access to a plurality of shared software objects by disparate entities as in claim 1 above, while neither of them explicitly discloses that the verification component employs operating system identities to facilitate security authorization procedures. However, Garg et al discloses a system to provide access control to individual properties of an object which, further discloses the verification component employs operating system identities to facilitate security authorization procedures (*security descriptor contains various properties including the owner security identifier and access control list) (column 8, lines27-30)*. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Beckwith et al and Koritzinsky et al such as to include a management portal. One would have been motivated to verify this in order to help maintain the integrity of the system by not

allowing changes to be made to the software by any entity, both known and unknown, scrupulous and unscrupulous.

12. Claims 18-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al (US 6,640,097) in view of Beckwith et al (US 6,330,598).

Claims 18: Corrigan et al discloses a method to facilitate security for subscription objects, comprising:

i. storing one or more security options in a database, the security options related to an

automated billing and provisioning system, wherein the security options include at least conversion of a subscription from a first type associated with a first tenant to a second type associated with a second tenant, wherein the security option indicates allowability of the second tenant to convert the subscription type from the first type to the second type (*a service conversion and message relaying platform between said interfaces for provision of internet content to mobile subscribers)(column 2, lines 5-7; column 3, lines 19-24)*;

ii. Assigning the security options to a class (*the platform comprises means for controlling mobile subscriber access according to the security criteria) (column 2, lines 9-15)*; and

iii. Inheriting the security options by object members of the class (*verification of subscriber access rights is an intrinsic part of the session management functions provided by the portal (column 9, lines 17-20*).

But does not explicitly discloses a step of storing one or more security options in a database, the security options related to an automated billing and provisioning system. However, Beckwith et al discloses a global service management system, which further discloses a step of storing one or more security options in a database, the security options related to automate billing and provisioning (the objects 84 in the automatic provisioning receiver class are capable of recording requests to add or delete services from subscription packages, to acknowledge that the requested service modification(s) (*be they adding a service to a subscription package or deleting a service from a subscription package) have been scheduled, and to deliver the requested service modification(s) to the appropriate objects for implementing the change(s)* (*column 3, lines 29-40; column 6, lines 5-9; column 7, lines 54-56; column 8, lins47-58*). Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention was made for Corrigan et al to include at least a step of converting a subscription type. One would have been motivated to do in order to make the system flexible.

Claim 19: Corrigan et al and Beckwith et al disclose a system to provide access control to individual properties of an object as in claim 18 above, and Corrigan et al further discloses that the system further comprises at least one of explicit and

implicit assigning the security options to object members of a class (*security future such as white list or blacklist are used to authenticates access to particular services (column 5, lines 27-30*).

Claim 20: Corrigan et al and Beckwith et al disclose a system to provide access control to individual properties of an object as in claim 18 above, and Corrigan et al further discloses that the system further comprises accessing database via an application programming interface *(in one embodiment, the portal comprises a secure web-bases self provisioning interface comprising means for setting mobile network subscribers to select a portfolio of personalized services (column 2, lines 53-57*).

Claim 21: Corrigan et al and Beckwith et al disclose a system to provide access control to individual properties of an object as in claim 20 above, and Corrigan et al further discloses a step of authorizing the API (*the node controls all subscriber accesses to the network operator managed service portfolio and authenticates the ID to verify that the subscriber is authorized (column 5, lines 33-38*).

Claim 22: Corrigan et al and Beckwith et al disclose a system to provide access control to individual properties of an object as in claim 21 above, and Corrigan et al further discloses that the system further comprises returning an error code if an authorization procedure fails (*the push server also support the push access protocol result notification. It will acknowledge successful or report unsuccessful transmission and delivery of the information pushed and return a status) (column 11, lines 10-15*).

Claim 23: Corrigan et al and Beckwith et al disclose a system to provide access control to individual properties of an object as in claim 21 above, and Corrigan et al further discloses a step of analyzing a simple object request (*a mobile user service request reaches the node as URL request in http format, and the node presents a login screen. The user inputs access security codes and the node interfaces on the Internet side to have the required content delivered) (column 4 lines 1-10*).

Claim 24: Corrigan et al and Beckwith et al disclose a system to provide access control to individual properties of an object as in claim 21 above, and Corrigan et al further discloses a step of analyzing one or more security credentials (*verification of subscriber access rights is an intrinsic part of the session management functions provided by the portal (column 9, lines 15-20*).

Claim 25: Corrigan et al and Beckwith et al disclose a system to provide access control to individual properties of an object as in claim 24 above, and Corrigan et al further discloses that the system further comprises employing a cache to process the credentials (*portal comprises a customer care provisioning interface and a provisioning database) (column 2, lines 65-68, Fig 2*)

Claim 26: Corrigan et al and Beckwith et al disclose a system to provide access control to individual properties of an object as in claim 18 above, and Corrigan et al further discloses that the system further comprises a subscription platform service (*the platform comprises means for controlling subscriber access according to security criteria (column 2, lines 5-10*).

Claim 27: Corrigan et al and Beckwith et al disclose discloses a system to provide access control to individual properties of an object as in claim 18 above, and further discloses that the security options are associated with default security parameters (*a generic subscriber class which is defined within the portal and represents common characteristics of all subscribers) (column 8, lines 44-48*).

Claim 28: Corrigan et al and Beckwith et al disclose discloses a system to provide access control to individual properties of an object as in claim 18 above, and Corrigan et al further discloses that the system further comprises overriding default security parameters with other options (*from the generic subscriber class are derived many subscriber sub-class that allow the portal to manage subscriber profiles across a wide range of different technologies) (column 8, lines 47-50*).

Claim 29: Corrigan et al and Beckwith et al disclose discloses a system to provide access control to individual properties of an object as in claim 18 above, and Corrigan et further discloses that the system further comprises employing an intermediate proxy that places call in a subscription on behalf of another tenant (*the wireless application protocol (WAP) is a complete WAP capable mobile stations to access applications and services which may be hosted either within the network operator's own domain or in another location (column 10, lines 50-55*).

13. Claims 31 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corrigan et al (US 6,640,097) in view of Beckwith et al (US 6,330,598).

Claim 31: Corrigan et al discloses a data packet stored on a computer readable storage medium that when transmitted facilitates communications between at least two components of an subscription platform service(*abstract),* comprising:

i. An Application Programming Interface packet to identify a first partner (*authenticates the subscriber ID to verify that the subscriber is authorized (column 5, lines 35-40*);

ii. A security credential packet to facilitate authorization of the first partner (*authorized subscriber access through white and black lists) (column 5, lines 50- 55*); and

iii. A security parameter packet inherited by a business object to facilitate access to a subscription platform database (*the data structure includes a identifier used to indicated a specific object property or set of properties to which the permission apply) (column 3, lines 35-40*),

but does not explicitly discloses wherein the security parameter packet includes at least a security parameter for conversion of a subscription of a subscriber from a second type associated with a second partner to a first type associated with the first partner, wherein the security parameter indicates allowability to the first type . However , Koritzinsky et al discloses an imaging system protocol handling method, which further discloses wherein the security parameter packet includes at least a security parameter for conversion of a subscription of a subscriber from a second type associated with a second partner to a first type associated with

the first partner, wherein the security parameter indicates allowability to the first type(column 21, line 33 to column 22 line 34).

Claim 32: Corrigan et al discloses a computer readable storage medium having a data structure stored thereon, the data structure comprising:

i. At least one security field indicating global security parameters in a subscription platform database (*authorized subscriber access through white and black lists) (column 5, lines 50-55)*, wherein the global security parameters include at least a security parameter for conversion of a subscription of a subscriber from a first type associated with a first tenant to a second type associated with a second tenant, wherein the security parameter for conversion indicates allowability of the second tenant to convert the subscription from the first type to the second type (*a service conversion and message relaying platform between said interfaces for provision of internet content to mobile subscribers)(column 2, lines 5-7; column 3, lines 19-24)*;

ii. At least one object field associated with an account in the database (*the portal comprises means for instantiating a payment management class) (column 3, lines 25-30)*; and

iii. At least one class field to associate the security field and the object field (*the data*

iv. *structure includes an identifier used to indicate a specific object property or set of properties to which the permission apply) (column 3, lines 35-40*).

but does not explicitly discloses wherein the global security parameters include at least a security parameter for conversion of a subscription of a subscriber from a first type associated with a first tenant to a second type associated with a second tenant, wherein the security parameter for conversion indicates allowability of the second tenant to convert the subscription from the first type to the second type. However , Koritzinsky et al discloses an imaging system protocol handling method, which further discloses wherein the security parameter packet includes at least a security parameter for conversion of a subscription of a subscriber from a second type associated with a second partner to a first type associated with the first partner, wherein the security parameter indicates allowability to the first type(column 21, line 33 to column 22 line 34).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone

number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

January 26, 2009

/F. T./

Examiner, Art Unit 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436